

Lythe Data Processing Addendum

Last updated: 21 October 2026

1. Scope and Application

This Data Processing Addendum (this “DPA”) forms part of the Fraser Simulation Studio Terms of Service, an Order Form, Master Services Agreement, pilot agreement, customer agreement, or other written agreement that incorporates this DPA (the “Agreement”) between the customer identified in the Agreement (“Customer”) and Lythe Inc., a Delaware corporation (“Lythe”), concerning Customer’s use of Fraser Simulation Studio and related Lythe services (the “Services”).

Lythe Inc. provides the Services to business customers in the United States at launch. Any affiliate engaged to Process Customer Personal Data must be disclosed and authorized under Section 8; an affiliate is not an active Subprocessor merely because it is named in an agreement. If an executed customer agreement separately identifies Lythe Pte. Ltd. as the contracting provider, references to Lythe mean that entity for that agreement. A United States customer location does not establish all data, Data Subject, provider, or transfer locations.

This DPA applies only to the extent Lythe Processes Customer Personal Data on behalf of Customer in connection with the Services. If there is a conflict between this DPA and the Agreement regarding the Processing of Customer Personal Data, this DPA controls to the extent of that conflict. Capitalized terms not defined in this DPA have the meanings given in the Agreement or applicable Data Protection Laws.

2. Definitions

“Applicable Data Protection Laws” means privacy, data protection, and data security laws applicable to the Processing of Customer Personal Data under the Agreement, including, where applicable, the GDPR, UK GDPR, Swiss Federal Act on Data Protection, Singapore Personal Data Protection Act 2012, California Consumer Privacy Act as amended by the California Privacy Rights Act, and other applicable U.S. state privacy laws.

“Customer Personal Data” means personal data, personal information, or similar regulated information included in Customer Data and Processed by Lythe on behalf of Customer through or in connection with the Services.

“Data Subject” means an identified or identifiable natural person to whom Customer Personal Data relates.

“GDPR” means Regulation (EU) 2016/679.

“Process,” “Processed,” or “Processing” has the meaning given under Applicable Data Protection Laws.

“Security Incident” means a breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by Lythe. Security Incident does not include unsuccessful attempts or activities that do not compromise Customer Personal Data, including pings, port scans, failed login attempts, denial-of-service attempts, or similar events.

“Subprocessor” means an affiliate or third party engaged by Lythe to Process Customer Personal Data on behalf of Customer in connection with the Services.

“Supervisory Authority” means an independent public authority responsible for enforcing Applicable Data Protection Laws.

“UK GDPR” means the GDPR as incorporated into United Kingdom law.

3. Roles and Instructions

3.1 Roles

Customer acts as controller or, where it Processes data for another controller, as processor with authority to appoint Lythe as a subprocessor. Lythe acts as processor or subprocessor accordingly. Where U.S. state privacy law or Singapore law applies, the corresponding statutory roles apply to the relevant Processing. Customer must obtain any required upstream authorization. Each party remains responsible for its own legal obligations. Lythe’s Processing of account, billing, security, and business-contact information for independently determined purposes is described in the Privacy Policy; this does not authorize repurposing Customer Personal Data or removing customer payloads from this DPA.

3.2 Documented Instruction

Lythe will Process Customer Personal Data only on Customer’s documented instructions, including the Agreement, this DPA, accepted Run Records and Data Approvals, configurations and Customer’s permitted use of the Services, and other written instructions accepted by Lythe, unless Processing is required by applicable law. If applicable law requires Processing outside Customer’s instructions, Lythe will notify Customer before Processing unless legally prohibited from doing so.

3.3 Lawful Instructions

Customer will ensure that its instructions and use of the Services comply with Applicable Data Protection Laws. Lythe will promptly inform Customer if, in Lythe’s reasonable opinion, an instruction infringes Applicable Data Protection Laws, and may suspend the affected Processing until the parties resolve the issue.

3.4 Customer Responsibilities

Customer must supply only Permitted Inputs under the Terms of Service and remain responsible for lawful source collection, required rights, notices, consents and lawful bases, minimization, any necessary anonymization and instructions. Necessary ordinary personal details incidental to authorized public-page evaluation may be processed within accepted scope. Real customer records, feedback or conversation materials require a separate Data Approval completed before Lythe receives or accesses them, including the required processing and transfer particulars. Lythe recommends synthetic sample records for authenticated testing. Safeguarded test accounts remain required; real customer records must remain hidden unless Lythe expressly approves the particular records, target access and safeguards in a Data Approval before receiving or accessing them. This DPA and Customer instructions do not authorize sensitive or otherwise prohibited information, profiling real people or data outside those boundaries.

4. Processing Restrictions

4.1 Purpose Limitation

Lythe will Process Customer Personal Data only to provide, operate, secure, support, troubleshoot, evaluate, and administer the Services; comply with Customer's instructions; prevent fraud and abuse; comply with law; and perform the Agreement.

4.2 No Sale or Sharing

Lythe will not sell Customer Personal Data, share Customer Personal Data for cross-context behavioral advertising, or retain, use, or disclose Customer Personal Data outside the direct business relationship with Customer, except as permitted by Applicable Data Protection Laws and the Agreement.

4.3 No Combining

Where required by applicable U.S. state privacy law, Lythe will not combine Customer Personal Data received from Customer with personal information received from or on behalf of another person, or collected from Lythe's own interaction with a Data Subject, except as permitted by law to provide the Services or for permitted security and business purposes.

4.4 No Model Training

Lythe will not use Customer Personal Data or identifiable inputs to train Lythe models, shared models, general-purpose models or systems for other customers, and will not permit third-party AI or model providers to use Customer Personal Data to train their models. Within a prior Data Approval, Lythe may label permitted feedback and use it through prompts, retrieval or configuration for that Customer's own synthetic personas and simulations, without model

training or profiling real individuals. Lythe may also label truly anonymized information and use aggregated or de-identified information that identifies neither Customer nor an individual for analytics, security, reliability, usage measurement and product improvement, subject to the Agreement and law.

4.5 Confidentiality

Lythe will ensure that personnel authorized to Process Customer Personal Data are subject to confidentiality obligations and receive appropriate privacy and security instructions.

4.6 Compliance Notification and Remediation

Lythe will notify Customer without undue delay if Lythe determines that it can no longer meet its obligations under applicable U.S. state privacy laws with respect to Customer Personal Data. Upon reasonable notice, Customer may take reasonable and appropriate steps to verify, stop, and remediate any unauthorized use of Customer Personal Data, subject to the confidentiality, security, audit, and cost conditions set out in this DPA.

For purposes of the CCPA and its implementing regulations, Customer discloses Customer Personal Data to Lythe only for the limited and specified business purposes stated in Section 4.1 and Schedule 1. Where Lythe acts as a service provider or contractor, Lythe will comply with all applicable provisions of the CCPA and its implementing regulations and provide the same level of privacy protection required of businesses for that Customer Personal Data. Lythe will reasonably cooperate with Customer in completing legally required consumer requests, cybersecurity audits, risk assessments, and automated decisionmaking technology obligations relating to Lythe's Processing. Customer's rights under Sections 4.6 and 12 permit reasonable and appropriate verification at least once every twelve (12) months where required by law, subject to Section 12's confidentiality, security, scope, and cost conditions.

5. Security Measures

5.1 Safeguards

Lythe will implement and maintain reasonable and appropriate administrative, technical, and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. The current measures are described in Schedule 2.

5.2 Security Program

Lythe may update its security measures from time to time, provided that updates do not materially reduce the overall level of protection for Customer Personal Data during the applicable term.

5.3 Customer Security

Customer is responsible for configuring its accounts, workspaces, permissions, integrations, credentials, retention settings, and uploads securely and for promptly notifying Lythe of suspected unauthorized access or misuse.

5.4 Customer Data Separation

Lythe will maintain reasonable controls designed to prevent unauthorized cross-customer access to or exposure of Customer Personal Data. Lythe will not intentionally disclose Customer Personal Data to another customer except at Customer's direction, through Customer-authorized integrations, or as otherwise permitted by the Agreement, this DPA, or applicable law.

5.5 Session Replay

Lythe uses consent-gated PostHog analytics and session replay on its landing website as a controller activity governed by the Privacy Policy and Cookie Policy, not as Customer Personal Data Processing under this DPA. If Customer enables PostHog or another analytics or replay integration inside the product, Customer contracts for and controls that integration under its own provider account. Customer must apply legally required consent controls and must mask or exclude passwords, payment information, authentication credentials, API keys, security codes, and other sensitive fields. Any Customer Personal Data Processed by Lythe in providing the integration remains subject to this DPA.

6. Security Incidents

6.1 Notification

Lythe will notify Customer without undue delay after becoming aware of a Security Incident affecting Customer Personal Data. Lythe will not defer initial notice until its investigation is complete or all details are confirmed. Initial information may be supplemented in phases without undue further delay. Notice will be sent to Customer's designated security or administrative contact.

6.2 Information

To the extent known and legally permitted, Lythe's notice will describe the nature of the Security Incident, categories of affected Customer Personal Data and Data Subjects, likely consequences, measures taken or proposed, and a contact for further information.

6.3 Cooperation

Lythe will take reasonable steps to contain, investigate, and remediate a Security Incident and will reasonably assist Customer with legally required notifications. Customer is responsible for determining whether notices to Data Subjects, regulators, or others are required, except where Lythe has an independent legal obligation.

6.4 No Admission

Notification of a Security Incident is not an acknowledgment of fault or liability.

7. Data Subject Requests

7.1 Customer Responsibility

Customer is responsible for responding to Data Subject requests relating to Customer Personal Data, including requests to access, correct, delete, restrict, object, or obtain a portable copy.

7.2 Assistance

Taking into account the nature of the Processing, Lythe will provide reasonable assistance through available product functionality and, where necessary, additional reasonable measures to help Customer respond to Data Subject requests.

7.3 Direct Requests

If Lythe receives a request directly from a Data Subject relating to Customer Personal Data, Lythe will, where legally permitted, direct the request to Customer or notify Customer and will not substantively respond except on Customer's instructions or as required by law.

8. Subprocessors

8.1 General Authorization

Customer provides general authorization for Lythe to engage Subprocessors to Process Customer Personal Data in accordance with this DPA.

8.2 Current Subprocessors

Customer authorizes only providers identified as authorized Subprocessors in the applicable Lythe Subprocessor List or otherwise expressly authorized under this DPA. A provider recorded solely as a service provider or customer-controlled integration is not authorized to Process Customer Personal Data as a Subprocessor by listing alone. Required purposes, data categories, and relevant locations must be disclosed before such Processing begins.

8.3 Subprocessor Obligations

Lythe will enter into written agreements with Subprocessors that impose data protection obligations appropriate to the Processing and no less protective in material respects than the obligations applicable to Lythe under this DPA. Lythe remains responsible for its Subprocessors' performance of those obligations to the extent required by Applicable Data Protection Laws.

Where a Subprocessor processes personal information subject to the CCPA as a service provider or contractor, Lythe will require a written contract that complies with the applicable CCPA and implementing-regulation requirements for service providers and contractors.

8.4 Changes

Lythe will give Customer written notice of a proposed new or replacement Subprocessor at least thirty (30) days before it begins Processing Customer Personal Data. Notice will identify the provider, purpose, and relevant processing locations and will be sent to Customer's designated contact or another expressly agreed notification channel. The public list will also be updated. A public-list update alone does not replace this notice. Any exceptional change must comply with Applicable Data Protection Laws and mandatory transfer terms.

8.5 Objection

Customer may object to a proposed new or replacement Subprocessor on reasonable data-protection grounds by notifying Lythe within fifteen (15) days after receipt of notice. The parties will work in good faith to resolve the objection, including by considering a commercially reasonable alternative. If it cannot be resolved before the proposed Processing begins, either party may terminate the affected portion of the Services in accordance with the Agreement and applicable mandatory transfer terms. The disputed Processing will not begin for that Customer pending resolution or termination. Payment and refund consequences follow the controlling Agreement; no automatic pro-rata refund arises under this paragraph. A discretionary refund requires Lythe's approval and, only where required by the controlling Agreement, the parties' written agreement. Refunds approved under the Fraser Refund Policy require no additional bilateral written agreement. Nothing in this paragraph limits a refund or remedy required by applicable law or an express controlling contractual provision.

9. International Data Transfers

9.1 Transfers

Customer authorizes Lythe and its Subprocessors to Process Customer Personal Data in the United States, Singapore, and other countries in which authorized Subprocessors operate, subject to this DPA and Applicable Data Protection Laws.

9.2 Transfer Safeguards

Where a transfer requires an approved transfer mechanism, the parties will use applicable standard contractual clauses, transfer addenda, contractual protections, adequacy decisions, or other recognized mechanisms.

9.3 EEA Transfers

For transfers of Customer Personal Data subject to the GDPR that require and are eligible to rely on this mechanism, the European Commission Standard Contractual Clauses in Implementing Decision (EU) 2021/914 (“EU SCCs”) are incorporated in full by reference, with only the selections and permitted supplementary information specified here. Module Two applies where Customer is a controller and Lythe a processor; Module Three applies where Customer is a processor and Lythe a subprocessor. Clause 7 applies. Clause 9(a), Option 2 applies, with thirty (30) days’ advance notice under Section 8. The optional independent dispute-resolution provision in Clause 11(a) is not selected; all mandatory provisions of Clause 11 apply. Clause 17, Option 1 selects Irish law, and Clause 18 selects Irish courts. Schedules 1, 2 and 4 and the completed Transfer Record supply the required Annex information. The competent authority is determined under Clause 13 as described in Schedule 4.

9.4 UK Transfers

For restricted transfers subject to the UK GDPR that rely on standard contractual clauses, the parties incorporate the ICO’s International Data Transfer Addendum, version B1.0 (the “UK Addendum”), including its Part 2 Mandatory Clauses in full, together with the EU SCCs selected in Section 9.3. The incorporated text is the official ICO UK Addendum (version B1.0). Schedule 4 and the completed Transfer Record supply its Part 1 table information. Its mandatory provisions govern interpretation, permitted amendments, and subsequent revisions; this DPA does not replace or modify them.

9.5 Swiss Transfers

For transfers subject to Swiss data protection law, references in the EU SCCs to the GDPR and European Union will be interpreted to include applicable Swiss law and Switzerland, and the competent authority will be the Swiss Federal Data Protection and Information Commissioner where applicable.

9.6 Supplementary Measures

Each party will reasonably cooperate in conducting transfer assessments and implementing supplementary measures where required by Applicable Data Protection Laws.

10. Deletion, Return, and Retention

10.1 During the Term

Customer may access, export, or delete certain Customer Personal Data through available product features, subject to the Agreement and applicable technical limitations.

10.2 Termination

Upon termination or expiration of the Agreement, Lythe will, at Customer's choice and subject to Applicable Data Protection Laws, delete or return Customer Personal Data in active systems, including existing active copies, within thirty (30) days. Copies in backups are governed by Section 10.3. Further storage is permitted only to the extent required by applicable law or under a specific, lawful, documented Customer instruction that identifies the continued Processing service, purpose and retention period; this DPA continues to apply to that Processing. Lythe will record the applicable basis, affected data, access restrictions and deletion date or legally required retention condition, notify Customer where legally permitted, and delete retained data when that basis ends. General security, fraud-prevention, compliance or business-continuity interests alone do not extend this deadline.

10.3 Backups

Customer Personal Data remaining in backups after deletion from active systems will remain protected, be put beyond ordinary operational use, and be permanently deleted or rendered irrecoverable under the documented backup-deletion cycle. Before the relevant Processing begins, Lythe must disclose and record the maximum backup-deletion period. That period must not exceed ninety (90) days after deletion from active systems unless applicable law requires longer storage or Customer specifically instructs a different lawful, defined period in writing. Security or disaster-recovery needs do not authorize an open-ended extension. Backup data may be restored only where necessary for disaster recovery or as required by law; after restoration, the relevant deletion instructions must be reapplied before restored data returns to ordinary operational use. Retention required by law remains limited and documented under Section 10.2.

10.4 Suppression Records

Lythe may retain limited suppression, security, billing or compliance records only to the extent permitted by Applicable Data Protection Laws for the relevant role and purpose. This paragraph does not create an additional exception to Sections 10.2 or 10.3 or authorize retaining Customer payloads for Lythe's independent purposes. Any Customer Personal Data retained on Customer's behalf remains subject to the applicable deletion instruction, this DPA and mandatory law. Records lawfully processed for Lythe's independently determined account, billing or security

purposes are governed by the Privacy Policy and must be limited to the necessary data, purpose and retention period.

11. Assistance and Compliance

11.1 Assessments

Taking into account the nature of the Processing and information available to Lythe, Lythe will provide reasonable assistance with data protection impact assessments, prior consultations, and similar obligations where required by Applicable Data Protection Laws and related to Lythe's Processing.

11.2 Regulatory Cooperation

Lythe will reasonably cooperate with Customer and competent Supervisory Authorities regarding Lythe's Processing of Customer Personal Data, subject to applicable law and confidentiality restrictions.

11.3 Compliance Information

Upon reasonable written request, Lythe will provide information reasonably necessary to demonstrate compliance with this DPA, which may include security documentation, policy summaries, questionnaire responses, or independent reports where available.

12. Audits

12.1 Audit Rights

Where required by Applicable Data Protection Laws, Customer may audit Lythe's compliance with this DPA no more than once annually, unless a Security Incident or regulator requires additional review. Customer will first use available documentation and questionnaires before requesting an on-site audit.

12.2 Conditions

Any audit must be conducted during normal business hours, on reasonable prior notice, without unreasonable disruption, and subject to confidentiality, security, and access restrictions. Customer may use an independent auditor that is not a Lythe competitor and is bound by confidentiality obligations.

12.3 Costs

Customer will bear its audit costs and reimburse Lythe for reasonable costs of supporting an audit beyond routine compliance assistance, unless an audit identifies a material breach by Lythe.

13. Liability

The liability of each party arising out of or relating to this DPA is subject to the exclusions and limitations of liability in the Agreement, except to the extent those limitations are prohibited by Applicable Data Protection Laws. Nothing in this DPA limits Data Subject rights or regulatory authority under applicable law.

14. Term and Termination

This DPA begins when it is incorporated into the Agreement and remains in effect for as long as Lythe Processes Customer Personal Data on behalf of Customer. Sections that by their nature should survive termination, including confidentiality, deletion, audit, transfer, and liability provisions, will survive as applicable.

15. General

Except for mandatory transfer-mechanism terms, the governing law and forum specified in the Agreement apply to this DPA. References to Ireland in Schedule 4 apply only to EU SCC Clauses 17 and 18 and do not establish the governing law or forum for the DPA as a whole.

15.1 Order of Precedence

If the EU SCCs, UK transfer addendum, or other mandatory transfer terms conflict with this DPA, the mandatory transfer terms control for the relevant transfer. Otherwise, this DPA controls over conflicting data protection terms in the Agreement.

15.2 Updates

Lythe may update this DPA to reflect changes in law, regulatory guidance, or the Services. Material changes will apply prospectively and will be notified as required by the Agreement or Applicable Data Protection Laws.

15.3 Electronic Acceptance

This DPA may be incorporated and accepted electronically through the Agreement, checkout flow, product interface, or an executed Order Form. Enterprise customers may request a countersigned copy.

15.4 Contact

Privacy and DPA inquiries may be sent to team@lythe.ai.

Schedule 1 - Details of Processing

1. Subject Matter and Duration

Lythe Processes Customer Personal Data within Permitted Inputs to provide the accepted Customer-specific evaluation or simulation Services. This may include ordinary personal details incidental and necessary to evaluate authorized public pages and real customer records, feedback or conversation information within a separate Data Approval completed before receipt or access. The accepted Run Record or Data Approval must identify applicable source, purpose, necessary data categories, individuals concerned, authorized providers, access, retention and transfer restrictions before the Processing begins. Lythe recommends synthetic sample records for authenticated testing. Safeguarded test accounts remain required; real customer records must remain hidden unless Lythe expressly approves the particular records, target access and safeguards in a Data Approval before receiving or accessing them. Sensitive and otherwise prohibited inputs remain excluded. Truly anonymous information is outside this DPA to the extent it is not personal data under applicable law. This DPA also protects unexpected or unauthorized personal information during restricted containment, investigation, return or deletion, for the agreed term and limited retention under Section 10 and mandatory law. Lythe's independently determined account, billing and website processing is governed by the Privacy Policy. No data approval authorizes real-person contact or real transactions at launch.

2. Nature and Purposes of Processing

Providing, operating, hosting, securing, supporting, troubleshooting, evaluating, and administering the Services.

Creating, configuring, running, and evaluating AI personas, subagents, simulations, automated evaluators, visual evaluations, bug-testing workflows, and reports.

Processing necessary ordinary personal details incidental to approved public-page evaluation and real customer records, feedback or conversation information within a Data Approval completed before receipt or access, including secure receipt or scoped access, storage and minimization for the accepted Customer-specific testing and evaluation. Approved feedback may also be labeled and used through prompts, retrieval or configuration for Customer's own synthetic personas and simulations. Record access does not by itself authorize persona enrichment or any purpose beyond its Data Approval. Unapproved or prohibited material may be handled only as necessary

to contain, investigate, secure, return or delete it; model or simulation processing of that material must stop.

Generating synthetic feedback, product critiques, usability findings, evaluation reports, bug-testing results, analytics, and related Outputs.

Providing integrations, account administration, billing, customer support, logging, monitoring, security, fraud prevention, abuse detection, and compliance.

Supporting customer-controlled product analytics and, where Customer lawfully enables them, session-replay integrations to the extent Lythe Processes Customer Personal Data in providing the integration.

Updating prompts, configurations, or workflows for Customer's own deployment without training shared or general-purpose models.

3. Categories of Data Subjects

Customer personnel, administrators, authorized users, contractors, and business contacts.

Individuals whose ordinary professional details are incidentally visible on authorized public pages and necessary for the accepted page or product evaluation, without profiling or targeting them.

Individuals represented in real customer records, feedback, transcripts or conversation information within a prior Data Approval, as specified by the source and data-subject categories in that approval. Individuals in unexpected or prohibited materials are covered only for restricted containment, investigation, return or deletion.

Website and application users whose account, device, browser, usage, interaction, or session replay data is collected through Lythe-operated environments.

4. Categories of Customer Personal Data

Names, business contact information, account information, identifiers, roles, and authentication-related metadata.

Prompts, scripts, instructions, AI persona configurations, simulation settings, evaluation criteria, and workflow data.

Product materials, websites, URLs, screenshots, prototypes, landing pages, product flows, APK files, files, records, and datasets.

Ordinary personal information necessary for the approved purpose, such as names, roles, professional photographs, bylines, business contact details, necessary ordinary customer-record fields and non-sensitive feedback or conversation content, only within accepted public-page

scope or a specific Data Approval. Audio or other recording formats require an enabled feature and specific approval. Prohibited or unapproved material remains limited to restricted containment, investigation, return or deletion.

Simulation inputs and outputs, AI persona responses, product critiques, usability observations, bug-testing results, evaluation scores, reports, and analytics.

IP addresses, device and browser information, logs, page activity, feature usage, navigation paths, interaction events, cookies, session identifiers, and session replay data.

Billing contacts, subscription identifiers, invoices, payment status, and limited payment tokens or transaction metadata.

5. Sensitive Data

Customer must not supply sensitive or special-category personal data as testing or persona-enrichment inputs, including health data, biometric identifiers, government identifiers, precise individual location, financial account data, children's data, or comparable regulated information. This DPA, a feature approval, or a Transfer Record does not waive that restriction. Unexpected receipt remains protected by this DPA to the extent applicable and must be handled under the restrictions above. Approved test-account credentials must use the secure mechanism specified in the Terms of Service. Lythe does not intentionally collect authentication secrets or payment-card credentials through session replay.

6. Processing Frequency

Continuous or intermittent, depending on Customer's use, configuration, uploads, integrations, simulations, and support requests.

7. Customer Instructions

The Agreement, this DPA, Customer's configuration and use of the Services, and other written instructions accepted by Lythe.

Schedule 2 - Technical and Organizational Measures

1. Access Control

Role-based access and least-privilege principles for production systems and Customer Personal Data.

Authentication controls for personnel and administrative access. Multi-factor authentication is not mandatory for production administrators in the current deployment.

Periodic review and revocation of access when no longer required.

2. Encryption and Transmission Security

Encryption in transit using industry-standard transport security.

Encryption at rest where supported and appropriate for the relevant storage system.

Secure management of credentials, secrets, and API keys.

3. Infrastructure and Application Security

Network, hosting, content-delivery, and web-security controls appropriate to the deployment.

Logging, monitoring, abuse detection, and alerting for suspicious or unauthorized activity.

Vulnerability management, security updates, dependency review, and remediation processes proportionate to risk.

Controls designed to prevent unauthorized cross-customer access or exposure.

4. Data Minimization and Privacy Controls

Collection and Processing limited to data reasonably necessary for the Services and Customer instructions.

Masking or exclusion of passwords, payment information, authentication credentials, API keys, security codes, and other sensitive fields from session replay.

Consent gating for analytics and session replay where required by applicable law.

Retention, deletion, export, and suppression controls as described in the Agreement and this DPA.

5. Personnel and Vendor Security

Confidentiality obligations for personnel with access to Customer Personal Data.

Privacy and security awareness appropriate to personnel roles.

Due diligence and contractual data protection obligations for relevant Subprocessors.

6. Incident Response and Continuity

Procedures for investigating, containing, remediating, and communicating Security Incidents.

Backup and recovery processes appropriate to the Services and deployment environment.

Business continuity and service restoration measures proportionate to operational risk.

7. Auditability

Logging and records appropriate to access, system activity, security events, and material configuration changes.

Reasonable documentation and compliance information made available as described in this DPA.

Schedule 3 - Authorized Subprocessors

The current authorized Subprocessors are identified in the then-current Lythe Subprocessor List, which is incorporated into this DPA by reference. That list is the authoritative provider disclosure and may be updated in accordance with Section 8. This Schedule does not maintain a separate static provider snapshot.

Customer-authorized integrations selected, configured, and controlled by Customer under Customer's own account or agreement may not be Lythe Subprocessors. Lythe will update the Subprocessor List where it independently engages an integration provider to Process Customer Personal Data on Lythe's behalf.

Schedule 4 - Transfer Information

1. Data Exporter

The Data Exporter is the Customer identified in the Agreement, acting as controller or processor as applicable. Before a transfer relying on the EU SCCs or UK Addendum begins, the parties must complete a written Transfer Record, incorporated into this Schedule, identifying Customer's full legal name, trading name if different, registered or main address, official registration number if any, privacy contact role and email, relevant activities, and controller or processor role.

2. Data Importer

The Data Importer is Lythe Inc., with a registered address at 2209 Van Ness Avenue, San Francisco, CA 94109, United States, unless the executed Agreement expressly identifies Lythe Pte. Ltd., Singapore, as the provider. Privacy contact: team@lythe.ai. The Transfer Record must identify the selected entity's verified full legal and trading names, registered address, official registration number if any, contact role and email, relevant activities, and processor or subprocessor role. These particulars must be completed before a transfer relying on this mechanism begins; the entity name and email alone do not complete them.

3. Transfer Details

Schedule 1 supplies the transfer's data subjects, data categories, subject matter, purposes, frequency, duration, and retention, as limited by Customer's permitted use and completed Transfer Record. Schedule 2 supplies the applicable technical and organizational measures. Schedule 3 identifies authorized Subprocessors; a copy or stable version reference must be retained with the acceptance record and subsequent notices. The Transfer Record must specify customer-specific restrictions, the prohibition on sensitive customer inputs and safeguards for any unexpected personal data, Subprocessor Processing subject matter, nature and duration, the binding start date, accepted DPA and transfer-term versions, and legally effective assent. No restricted transfer may rely on incomplete required particulars or unverified safeguards. For UK Table 1, party details, contacts, start date and assent are supplied by this Schedule and the Transfer Record; Table 2 adopts the selections in Section 9.3; Table 3 uses this Schedule and Schedules 1–3 for the required Appendix information. For Table 4, both Importer and Exporter may exercise the termination right in Section 19 of the approved UK Addendum. The UK Addendum's mandatory provisions remain unmodified.

4. Competent Supervisory Authority

The competent Supervisory Authority is determined in accordance with the EU SCCs based on Customer's establishment, representative, and affected Data Subjects. Where the UK GDPR applies, the competent authority is the UK Information Commissioner. Where Swiss law applies, the competent authority is the Swiss Federal Data Protection and Information Commissioner.

5. Governing Law and Forum

For Clause 17 of the EU SCCs, Option 1 is selected and Irish law applies.

For purposes of Clause 18 of the EU SCCs, the parties submit to the jurisdiction of the courts of Ireland.

The competent Supervisory Authority under Annex I.C is determined under Clause 13 for the Data Exporter, considering its establishment, representative where applicable, and relevant Data Subjects. The Transfer Record must identify the authority and selection basis. Irish governing law or courts do not independently determine supervisory competence. The UK Addendum applies the law and courts of England and Wales, subject to its mandatory provisions and any alternative selection expressly permitted by it. Swiss adaptations apply where required without limiting mandatory Data Subject rights.